UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/306,227	05/06/1999	ROY CALLUM	042390.P6761	3173

7590 05/04/2004

CHARLES A MIRHO INTEL CORPORATION
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
12400 WILSHIRE BOULEVARD
7TH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	**PAPER NUMBER**
2131	10

DATE MAILED: 05/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/306,227	CALLUM, ROY	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed on February 17, 2004 have been fully considered but they are not persuasive.

It is argued by the applicant that Hardy et al fails to disclose of disabling a circuit when operating conditions have been altered beyond a predetermined range. The examiner respectfully disagrees for it is disclosed by Hardy et al that the operating conditions fall between a maximum and minimum value and when it is detected that the operating conditions are outside of those values, the circuit is disabled. Please refer to the rejection as is recited below.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1,2,4-6,16, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardy et al in view of Sebaa.

As per claims 1 and 4, it is shown in Figure 1 of Hardy et al of an operation unit adapted to perform a circuit operation in a plurality of state vectors (rounds)(col. 3, lines

11-19). The encryption algorithm is adapted to generate a unique set of state vectors at various points in the execution of encryption algorithms and the state vectors (rounds) are used to inform the state monitor that specific sections of the selected software encryption algorithm have been executed (col. 3, lines 27-34). A state monitor compares the state vectors with predetermined (reference value identifying the correct value) state vectors (col. 3, lines 44-50). A comparator checks the operations so that they fall between a minimum and maximum threshold value (predetermined range of operating conditions)(col. 4, lines 1-4). The examiner is interpreting the exceeding of the threshold value as a value that operates beyond the predetermined range, that is exceeding the minimum and maximum threshold values. A disablement signal is produced causing the flow of cipher text to stop when there is a miscomparison of the data (col. 12, lines 30-36). The teachings of Hardy et al are silent in disclosing of selecting between an receiving an input signal and a test signal and performing a test round of the circuit operation when the test signal is selected. Sebaa discloses of a circuit comprising two modes of operation, one being a normal mode (input signal) and the other being a (selected) test mode (test signal) which is performed on the circuit to determine if it is operating properly by generating signal sequences (test rounds)(col. 2, lines 43-61). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply Sebaa as a means of initiating testing of circuit to determine if it is operating properly. Sebaa recites motivation for this concept by reciting of detecting timing faults within the chip and it saves time and money to determine if it is operating improperly (col. 11, line 63 through col. 12, line 18).

It would have been obvious that the teachings of Hardy et al would have benefitted from the teachings of Sebaa as a means of integrating testing within the device by switching from a normal mode and a test mode to save time and money by eliminating the need for extra hardware as is taught by Sebaa.

As per claim 2, it is disclosed by Hardy et al that the circuit operation includes encryption (col. 2, lines 13-16).

As per claim 5, Hardy et al recites of generating a state vector (round) and making it available to the state monitor. A key (signal) is used for the encryption algorithm (col. 6, lines 10-19). It is taught that the circuit operation includes encryption (col. 2, lines 13-16).

As per claim 6, Hardy et al discloses of key (signal) which is used for the encryption algorithm (col. 6, lines 10-19). The examiner asserts that a first clock signal is used since the teachings of Hardy et al perform the monitoring based on normal operating conditions.

As per claims 16 and 17, it is disclosed by the teachings of Sebaa that the operating conditions include an operating clock frequency (col. 2, lines 49-51).

4. Claims 3 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardy et al in view of Sebaa in further view of Curiger et al.

As per claims 3 and 7, Hardy et al recites of generating a state vector (round) and making it available to the state monitor. A key (signal) is used for the encryption algorithm (col. 6, lines 10-19). The examiner asserts that a first clock signal is used since the teachings of Hardy et al perform the monitoring based on normal operating

conditions. The combination of the teachings of Hardy et al and Sebaa are silent in disclosing of providing a subsequent clock signal. It is disclosed by Curiger et al of known techniques in the prior art whereby an increased frequency (subsequent clock signal) is applied to an integrated circuit (col. 1, lines 34-37). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply means to detect different clocking signals. Curiger et al recites motivation for this concept by reciting that increased frequency (subsequent clock signals) can cause a circuit to operate improperly and calculation errors may result (col. 1, lines 34-38). The detection of this change of clock signals would have been beneficial to the combination of the teachings of Hardy et al and Sebaa as a means to ensure that the encryption operations are properly computed as is taught by Curiger et al.

5. Claims 8,9,11-15,18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardy et al in view of Curiger et al.

As per claims 8 and 13, it is shown in Figure 1 of Hardy et al of an operation unit adapted to perform a circuit operation in a plurality of state vectors (col. 3, lines 11-19). The encryption algorithm is adapted to generate a unique set of state vectors at various points in the execution of encryption algorithms and the state vectors are used to inform the state monitor that specific sections of the selected software encryption algorithm have been executed (col. 3, lines 27-34). A state monitor (sampling unit) compares the state vectors with predetermined state vectors (stored in memory)(col. 3, lines 44-50). A comparator (analytical unit) checks the operations so that they fall between a

minimum and maximum threshold value (col. 4, lines 1-4). The examiner is interpreting the exceeding of the threshold value as a value that operates beyond the predetermined range, that is exceeding the minimum and maximum threshold values. A disablement signal is produced causing the flow of cipher text to stop when there is a miscomparison of the data (col. 12, lines 30-36). The examiner asserts that a first frequency sample is used since the teachings of Hardy et al perform the monitoring based on normal operating conditions. The teachings of Hardy et al are silent in disclosing of applying a second frequency by means of an oscillator. The teachings of Curiger et al disclose of increasing an input clock frequency (second frequency sample) in order to stress the circuitry (col. 4, lines 15-19). An oscillator increases the frequency (to create additional values)(col. 5, lines 1-6). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply different frequency samples in order to test the circuitry for proper operations. Curiger et al recites motivation for this concept by reciting that increased frequency (subsequent clock signals) can cause a circuit to operate improperly and calculation errors may result (col. 1, lines 34-38). The detection of this change of clock signals would have been beneficial to the teachings of Hardy et al as a means to ensure that the encryption operations are properly computed as is taught by Curiger et al.

As per claims 9 and 14, Hardy et al discloses of a counter which counts the tasks (oscillations) which are performed (col. 11, lines 17-19). Curiger et al is relied upon for the disclosure of a second frequency, please refer to above for motivation of combining to the teachings of Hardy et al.

As per claim 11, it is taught by Hardy et al of subtracting (by a subtractor) the differences of the circuit performance levels (col. 8, lines 42-44). The teachings of Curiger et al are relied upon for the disclose of multiple frequency samples, please refer to the rejection above for the motivation of combining the teachings of Curiger to Hardy et al.

As per claim 12, Hardy et al disclose of a (magnitude) comparator which checks the operations so that they fall between a minimum and maximum threshold value (col. 4, lines 1-4). The teachings of Curiger et al are relied upon for the disclose of multiple frequency samples, please refer to the rejection above for the motivation of combining the teachings of Curiger to Hardy et al.

As per claim 15, the examiner asserts that a first frequency sample is used since the teachings of Hardy et al perform the monitoring based on normal operating conditions at the start of circuit operations. Curiger et al is relied upon for increasing an input clock frequency (second frequency sample) in order to stress the circuitry (col. 4, lines 15-19), please refer to the rejection above for the motivation of combining the teachings of Curiger to Hardy et al.

As per claims 18 and 19, it is disclosed by the teachings of Curiger et al that the operating conditions include an operating clock frequency (col. 5, lines 37-39).

6. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hardy et al in view of Curiger et al in further view of Mertel et al.

Hardy et al discloses of the use of a counter, but the combination of the teachings of Hardy et al and Curiger is silent in disclosing that the counter is a Johnson

counter. It is disclosed by Mertel et al of a counter which is a Johnson counter (col. 5, lines 5, lines 30-31). I would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a Johnson counter as a specific counter. Mertel et al discloses the benefits of a Johnson counter by reciting that it is used to identify specific master clock cycles and initiate various actions. The advantage of this particular type of counter is that is does not require numerous decode gate to identify cycles which saves hardware (col. 5, lines 6-12). It is obvious that the combination of the teachings of Hardy et al and Curiger et al would have benefitted from the use of a Johnson counter as per the advantages recited by Mertel et al.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 703-305-1843. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CR

May 4, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100